



Die Zukunft des Datenschutzbeauftragten

DATENSCHUTZMANAGEMENT *Die Alarmglocken schrillten bei Deutschlands Datenschützern kurz vor Weihnachten 2015. Es drohte dem Datenschutzbeauftragten der Garaus durch die EU. Doch die Angst war unbegründet. Im Gegenteil: Das Amt wurde nicht abgeschafft, sondern aufgewertet.*

VON THILO WEICHERT



Der betriebliche und behördliche Datenschutzbeauftragte ist im Text der künftigen Datenschutzregelung – der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) prominent und umfassend in den Artikeln 35 bis 37 (künftig 37 bis 39) geregelt.¹ Tatsächlich wird die EU-Verordnung, die europaweit im Jahr 2018 in Kraft treten soll, den Beauftragten für den Datenschutz aufwerten. Er ist eine deutsche Erfindung und hat sonst in der EU als verbindliches Instrument noch keine Verbreitung gefunden. Das sollte und wird sich ändern.

Art. 35 Abs. 1 verpflichtet nicht nur Behörden und andere öffentliche Stellen, sondern alle Unternehmen, deren »Kerntätigkeit« wegen der Art, des Umfangs und des Zwecks der Datenverarbeitung zu einer »systematischen Beobachtung« von Personen führt oder in der Verarbeitung besonders sensibler Daten besteht. Eine Unternehmensgruppe – also ein Konzern – darf einen gemeinsamen Datenschutzbeauftragten benennen, »sofern er von jeder Niederlassung aus [...] leicht erreicht werden kann«. Die in großen Unternehmensverbänden praktizierte Einrichtung eines gemeinsamen Konzerndatenschutzbeauftragten mit einem ganzen Team von Mitarbeitern kann also beibehalten werden. Diesem kommt dann auch bei der Etablierung und Durchsetzung von Binding Corporate Rules, Art. 42 Abs. 2, eine wichtige Funktion zu.

Bestellpflicht

Unabhängig von der Pflicht zur Bestellung bei den genannten Formen der Verarbeitung sieht Art. 35 Abs. 4 vor, dass zudem nicht nur eine freiwillige Bestellung möglich ist, sondern dass die Mitgliedsstaaten zusätzliche Pflichten zur Bestellung vorsehen können. Dies bedeutet: Die Befürchtung, dass der betriebliche Datenschutzbeauftragte der europäischen Harmonisierung geopfert wird, ist unbegründet. Vielmehr kann das deutsche System beibehalten werden – ja mehr als das, auch in anderen Ländern werden bestimmte Unternehmen (und alle Behörden) verpflichtet, einen Datenschutzbeauftragten zu bestellen. »Kerntätigkeit« bedeutet, so erläutert uns das der Erwägungsgrund 75 (97) der EU-DSGVO, die »Haupttätigkeit« einer Stelle, nicht deren Nebenaktivitäten.

DARUM GEHT ES

- 1.** Der betriebliche und behördliche Datenschutzbeauftragte ist die zentrale Stelle im Datenschutzmanagement.
- 2.** Der neue EU-Datenschutz stärkt die Stellung des Beauftragten für den Datenschutz.
- 3.** Der nationale Gesetzgeber hat jetzt seine Aufgaben – und seine Beziehung zur Arbeitnehmervertretung – zu konkretisieren.

¹ Vgl. Rat der Europäischen Union, Vorschlag für eine Datenschutz-Grundverordnung, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN

BINDING CORPORATE RULES

Binding Corporate Rules (BCRs) werden innerhalb von internationalen Konzernen mit Niederlassungen außerhalb der EU festgelegt, um konzernintern den Datenaustausch zu ermöglichen und gleichzeitig den Datenschutz – insbesondere auch die Betroffenenrechte der Beschäftigten – zu sichern. Werden BCRs von der zuständigen Datenschutzaufsichtsbehörde genehmigt, dann sind sie – bis zu ihrer förmlichen Aufhebung – verbindlich, so dass damit auch Datenübermittlungen in die USA legitimiert sind, wo Geheimdienste auf die Daten praktisch ungehindert zugreifen dürfen.

Bei Arbeitgebern gehört die Personaldatenverarbeitung wohl in jedem Fall zur Kerntätigkeit, so dass bei Vorliegen der Voraussetzungen (sensible Daten, systematische Überwachung) eine Bestellpflicht besteht:

Das ist der Fall, wenn die Kerntätigkeit die Verarbeitung von Daten zur Gesundheit, zum Sexualleben, zur rassischen und ethnischen Herkunft, zu religiösen und weltanschaulichen Überzeugungen und zur Gewerkschaftszugehörigkeit mit umfasst. Hinzu gekommen sind weitere besonders geschützte Datenarten, die auch die Bestellpflicht auslösen: genetische und biometrische Daten sowie Daten zu Strafverfahren, vergleiche Art. 9, 9a. Es genügt schon, dass diese Daten auch verarbeitet werden.

Etwas mehr Interpretationsaufwand ist bei dem Kriterium der »umfangreichen, regelmäßigen und systematischen Beobachtung von betroffenen Personen« gefordert. Der EU-Gesetzgeber hat hier wohl vorrangig die Internet-Überwachung vor Augen gehabt, also etwa das Profiling von Internet-Usern, das Scoring im Bereich von Auskunfteien oder Big Data-Auswertungen von Konsumenten. Doch auch die systematische Überwachung von Beschäftigten erfüllt den Tatbestand. Diese findet schon statt, wenn Beschäftigte zum Beispiel dauernder Videoüberwachung ausgesetzt sind, aber erst Recht, wenn sie bezüglich ihrer Leistung und ihrem Verhalten digital kontrolliert werden.

Davon unabhängig darf der deutsche Gesetzgeber seine bisherigen Regelungen zur Bestellpflicht beibehalten. Nach § 4f Abs. 1 des Bundesdatenschutzgesetzes (BDSG) besteht diese derzeit ab zehn Personen bei automatisierter Datenverarbeitung beziehungsweise ab 20 Beschäftigten, die mit personenbezogenen Daten regelmäßig zu tun haben. Diese Bestellpflicht ist in Deutschland nicht (mehr) umstritten. Es sollte deshalb ein Selbstläufer sein, dass diese Regelung beibehalten bleibt, wenn das bisherige BDSG durch ein Ausführungsgesetz zur EU-DSGVO abgelöst wird.

Voraussetzung und Aufgaben

Die konkrete Ausgestaltung der Funktion des Datenschutzbeauftragten in der EU-DSGVO erinnert stark an die bestehende Regelung gemäß dem deutschen BDSG: Der Beauftragte soll mit seinem Fachwissen im Bereich des Datenschutzrechts und der Datenschutzpraxis

besonders beruflich qualifiziert sein. Möglich sind sowohl eine interne wie eine externe Bestellung. Denkbar dürfte auch sein, dass über gemeinsame Verhaltensregeln in Branchen insbesondere für kleinere Unternehmen eine Bündelung erfolgt, Art. 40 Abs. 1. Name und Kontaktdaten sind der zuständigen Aufsichtsbehörde bekanntzugeben und beispielsweise

»Der Datenschutzbeauftragte soll also die zentrale Stelle im Datenschutzmanagement einer Behörde oder eines Unternehmens sein.«

THILO WEICHERT

auf der Website des Unternehmens zu veröffentlichen, Art. 35 Abs. 5–7.

Funktion des Beauftragten ist es, die jeweilige verantwortliche Stelle oder den Auftragsdatenverarbeiter in allen Fragen des Datenschutzes zu unterstützen, was eine enge Kommunikation mit der Stellen- oder Unternehmensleitung voraussetzt, Art. 36 Abs. 1, 2. Diese Funktion wird durch die Wahrnehmung folgender Aufgaben erfüllt:

Unterrichtung und Beratung der Stellenleitung und der Beschäftigten, Kontrolle, Schulung, Unterstützung bei der »Datenschutz-Folgenabschätzung«, Zusammenarbeit mit der Aufsichtsbehörde und Bearbeitung der Datenschutzkommunikation, wozu die Behandlung von Beschwerden und Anfragen von Betroffenen gehört, Art. 37 Abs. 1, 36 Abs. 2a. Auch künftig können der anlasslos zulässigen Kontrolle durch den Datenschutzbeauftragten im Betrieb keine Berufs- und auch keine Betriebs- und Geschäftsgeheimnisse entgegengehalten werden. Zu den Beratungs- und Berichtspflichten gehörten in der Vergangenheit in der

Praxis regelmäßige Tätigkeitsberichte. Daran muss sich nichts ändern.

Der Datenschutzbeauftragte soll also die zentrale Stelle im Datenschutzmanagement einer Behörde oder eines Unternehmens sein. Die Zuordnung zur »höchsten Managementebene« ist auch künftig gewährleistet, Art. 36 Abs. 3 Satz 3. Eine darüber hinausgehende umfassende Regelung des Datenschutzmanagements ist nicht erfolgt. Wohl aber gibt es neue Instrumente, so neben der Folgenabschätzung insbesondere die Durchführung von Zertifizierungen und der Erwerb von Siegeln und Prüfzeichen, Art. 39.

Zu den Datenschutzpflichten gehört künftig nicht mehr nur die Beachtung des materiellen Rechts, der Betroffenenansprüche (Art. 14 ff.) und die Umsetzung des technischen Datenschutzes (Art. 23, 30), sondern auch die des Grundsatzes der Datenminimierung, der prominent in Art. 5 Abs. 1 c sowie in mehreren Spezialregelungen in die Verordnung Eingang gefunden hat. Spezifische Aufgaben bleiben das Führen von einem »Verzeichnis von Verarbeitungstätigkeiten« (Art. 28) und die »Breach Notification«, also die Unterrichtung über Datenschutzverstöße (Art. 31 f.).

Anstelle der bisher stark bürokratisierten Vorabkontrolle stellt die EU-DSGVO nun eine risikoorientierte »Datenschutz-Folgenabschätzung«² in den Vordergrund, Art. 33 f. Dabei hat die Stelle unter Einbeziehung des Datenschutzbeauftragten beim Gebrauch neuer Technologien eine Bewertung der Konsequenzen des Einsatzes auf den Datenschutz vorzunehmen. Als risikoträchtig wird die »systematische und umfassende Bewertung persönlicher Aspekte« angesehen, wozu auch das Profiling zählt, das Verarbeiten sensibler Daten und die »systematische weiträumige Überwachung öffentlich zugänglicher Räume«. Die Aufsichtsbehörden können die Voraussetzungen für die Folgenabschätzung konkretisieren und ausweiten.

Diese Abschätzung beinhaltet eine systematische Dokumentation der Verfahren, eine Bewertung der Erforderlichkeit, auch unter dem Aspekt der Datenminimierung, eine Risikoabschätzung sowie eine Darstellung der »Abhilfemaßnahmen«, also der Garantien, Sicherheitsvorkehrungen und Verfahren, mit denen ein angemessener Datenschutz erreicht werden soll.

Dabei sind nicht nur die gesetzlichen Regelungen, sondern auch möglicherweise beste-

hende Verbands-Verhaltensregeln zu berücksichtigen.

Eine Verpflichtung durch die Aufsichtsbehörde gegenüber dem Unternehmen zur Abberufung des Beauftragten für den Datenschutz bei fehlender Fachkunde und Zuverlässigkeit, wie sie bisher in § 38 Abs. 5 Satz 3 BDSG vorgesehen ist, ist in der EU-DSGVO nicht geregelt. Da aber sowohl die Ausgestaltung der Befugnisse der Aufsichtsbehörden wie auch des Datenschützers dem nationalen Gesetzgeber weiter zugestanden bleibt, kann diese Norm in einem EU-DSGVO-Ausführungsgesetz beibehalten werden. Die berufsrechtlichen Voraussetzungen an die Qualifikation des Datenschutzbeauftragten könnten und sollten aber näher präzisiert werden, zumal dessen praktische Aufgaben weiter zunehmen und anspruchsvoller werden.

Stellung

Die Wahrnehmung der Aufgaben soll, wie bisher nach deutschem Recht, unabhängig erfolgen. Wegen der Ausübung seines Amtes darf er nicht abberufen oder benachteiligt werden. Der bisher geltende Kündigungsschutz analog § 626 des Bürgerlichen Gesetzbuchs (BGB) in § 4 f Abs. 3 Satz 4–6 BDSG steht damit in Einklang. Dem Datenschutzbeauftragten dürfen zur Amtsausübung keine Anweisungen erteilt werden.

Um seine Funktion effektiv wahrnehmen zu können, ist der Beauftragte bei allen Datenschutzfragen von Anfang an einzubinden. Ihm sind die nötigen Ressourcen zur Verfügung zu stellen. Er ist zur Geheimhaltung und zur Vertraulichkeit verpflichtet. Seine Aufgaben müssen nicht hauptberuflich wahrgenommen werden, das heißt das Befassen mit anderen Aufgaben und Pflichten ist zulässig, wobei dies aber nicht zu Interessenkonflikten führen darf. In Bezug auf die Haftung der Datenschutzbeauftragten wird sich, weil die EU-DSGVO nun für den betrieblichen Datenschützer vergleichbare Handlungspflichten wie bisher im BDSG vorsieht, in Deutschland nichts wesentlich ändern.³

Nicht nur im Hinblick auf die Bestellpflicht, wohl auch in Bezug auf die Konkretisierung der Aufgaben und der Stellung des Beauftragten hat der nationale Gesetzgeber die Möglichkeit der weiteren normativen Konkretisierung. Dies hat zum Beispiel zur Folge,

DATENSCHUTZBEAUFTRAGTE

CuA-Artikelreihe zum
Datenschutzbeauftragten

Bruno Schierbaum, Der betriebliche/ behördliche Daten- schutzbeauftragte

Teil 1: Bestellung, Abberufung und Kündigungsschutz, in: CuA 3/2010, 15 ff.

Teil 2: Voraussetzungen, Stellung und Unterstützungspflicht, in: CuA 4/2010, 24 ff.

Teil 3: Aufgaben und Befugnisse, in: CuA 5/2010, 24 ff.

Teil 4: Zusammenarbeit mit der Interessenvertretung, in: CuA 6/2010, 21 ff.

² Ausführlich dazu Wedde, Datenschutzrecht für »Europa 4.0«, in: CuA 3/2016, 8 ff.

³ Sander, Die Haftung des Datenschutzbeauftragten unter Berücksichtigung der EU-DSGVO, in: BvD-News 1/2016, 16 f.

AUFGABEN UND BEFUGNISSE

Die Datenschutzbeauftragten in Behörde und Betrieb

Eine aktuelle Broschüre der Bundesdatenschutzbeauftragten informiert über Bestellung, Befugnisse und Aufgaben von internen Datenschutzbeauftragten. Sie stellt die wichtigsten Rechtsvorschriften vor, verbunden mit einführenden Erläuterungen und praktischen Hinweisen.

www.bfdi.bund.de

(> Infothek > Informationsmaterial)

dass die Regelungen zur Verschwiegenheit in § 203 Abs. 2a des Strafgesetzbuchs (StGB) und zum Zeugnisverweigerungsrecht in § 4f Abs. 4a BDSG beibehalten werden können, vgl. Art. 84 Abs. 1.

Konkretisierungsbedürftig und -fähig ist die Beziehung des betrieblichen Datenschützers zum Betriebsrat. In Art. 82 wird den Mitgliedsstaaten das Recht zugesprochen, die Datenverarbeitung im Beschäftigtenkontext und damit auch die Beziehung zum betrieblichen Datenschützer national zu regeln; Konkretisierungen sind insofern auch auf der Ebene der Tarifparteien oder der Betriebe durch Vereinbarungen mit der Beschäftigtenvertretung möglich. Ein Betriebsratsratsmitglied kann grundsätzlich auch weiterhin zugleich Datenschutzbeauftragter sein.⁴

Ausblick

Nach der förmlichen Verabschiedung der EU-DSGVO beginnt erst einmal die Arbeit der nationalen Gesetzgeber. Der Bundestag (und auf Landesebene auch die Landesparlamente) müssen das bestehende Datenschutzrecht an die EU-DSGVO-Regelung anpassen, die ja – anders als bisher die Europäische Datenschutzrichtlinie – direkt und verbindlich anwendbar ist. Regelungsspielraum besteht noch dort, wo – wie beim Beschäftigtendatenschutz oder beim beruflichen Geheimnisschutz – Öffnungsklauseln bestehen sowie hinsichtlich der Konkretisierung der teilweise sehr offen formulierten Regelungen. Zu empfehlen ist insofern, die Mitbestimmungspflicht bei der Bestellung des Beauftragten für den Datenschutz einzuführen.

Da zu erwarten ist, dass der Bundesgesetzgeber die weitergehende Bestellpflicht beim betrieblichen und behördlichen Datenschützer beibehalten wird und für das Regelungskonzept der EU-DSGVO viele Anleihen beim deutschen Vorbild genommen wurden, wird sich kurz- wie mittelfristig für die konkrete Arbeit des Datenschutzbeauftragten im Betrieb und in der Beziehung zu den Beschäftigten und deren Vertretung voraussichtlich nicht viel ändern.

Angesichts des Umstands, dass der deutschen Bundesregierung aber der Datenschutz derzeit nicht allzu wichtig zu sein scheint, muss von Datenschutz- und Beschäftigtenseite

die anstehende nationale Gesetzgebung aufmerksam und kritisch begleitet werden.⁵

Während es in Bezug auf den Beauftragten und seine Funktion wenig Änderungen mit der EU-Verordnung geben wird, so gilt dies nicht für die materiellen Regelungen. Insofern haben wir es künftig mit einer neuen Normstruktur und oft neuen Norminhalten zu tun. Die erweiterten Betroffenenrechte sind in der EU-DSGVO abschließend geregelt. Und der gesamte Aufsichtsmechanismus mit den Datenschutzbehörden unterliegt einem gewaltigen Umbruch.

Nach der Aufhebung von Safe Harbor durch den Europäischen Gerichtshof (EuGH)⁶ und den dabei konkretisierten Voraussetzungen für den grenzüberschreitenden Datentransfer in Länder ohne angemessenen Datenschutz kommen auf Belegschaftsvertretung und Datenschutzbeauftragten gemeinsam neue Herausforderungen zu.

Nachdem klar ist, dass die Vorschläge der EU-Kommission für einen sogenannten EU-US-Privacy-Shield absolut unzureichend sind, muss sich der Datenschützer darum kümmern, dass die internationale Kommunikation auf eine datenschutzkonforme Grundlage gestellt wird, beispielsweise indem die Unternehmen jeweils einen Export-Import-Vertrag mit ihren ausländischen Kooperationspartnern abschließen.⁷

Angesichts der weiter gehenden Digitalisierung in den Unternehmen wird die Bedeutung des Datenschutzbeauftragten zunehmen. Das kann und darf die Arbeitnehmerseite nicht links liegen lassen; das heißt der Austausch und die Kooperation mit ihm sollten intensiviert werden, soweit dies möglich ist. Stoßen Beschäftigte und ihre Interessenvertretung hier auf Schwierigkeiten beim Beauftragten selbst oder bei der Unternehmensleitung, so sollten sie sich nicht scheuen, die Hilfe der örtlichen Datenschutzbehörde in Anspruch zu nehmen. ◀



Thilo Weichert, Mitglied des »Netzwerks Datenschutzexpertise«
weichert@netzwerk-datenschutz-expertise.de

Thilo Weichert war von 2004 bis 2015 Leiter des Unabhängigen Landesentrums für Datenschutz Schleswig-Holstein.

⁴ Däubler/Klebe/Wedde/Weichert, BDSG, 5. Auflage 2016, § 4f Rn. 32 und Däubler, Datenschützer als Verbündeter?, in: CuA 4/2016, 13 ff., in diesem Heft

⁵ Der DGB fordert ein separates Beschäftigtendatenschutzgesetz, siehe CuA-Redaktion, »Der Kampf wird sich lohnen«, in: CuA 3/2016, 20 ff.,

⁶ Siehe dazu Weichert, Das Safe Harbor-Urteil und die Folgen, in: CuA 2/2016, 8 ff.; EuGH 6.10.2015 – Rs. C-362/14, <http://curia.europa.eu/juris/documents.jsf?num=C-362/14>

⁷ Dazu Netzwerk Datenschutzexpertise, Folgen der Safe Harbor-Entscheidung, www.netzwerk-datenschutzexpertise.de/dokument/folgen-der-safe-harbor-entscheidung-des-eugh-privacy-shield

